Y2K AND EPA EMERGENCY RESPONSE

- a general impact discussion -

PURPOSE

This white paper was developed by the EPA Region 9 Office of Emergency Response and EPA OERR to contribute to a focused discussion of the potential impact of the Y2k technology problem on the EPA removal program and emergency response capabilities. It was also developed to provide input for on-going contingency planning efforts. It is a living document and will be edited and up-dated from time to time as feedback is received. It is important to note that the contents and references contained in the paper are believed by the authors to be accurate at the time of publication. However, information on Y2k is very fluid and is constantly being revised and updated. Readers are advised to consult the most recently available information from reliable sources in pursuing an education on Y2k.

INTRODUCTION

Y2k, a.k.a the year 2000 technology problem, a.k.a. the millennium bug, a.k.a. overblown, a.k.a. under-estimated, a.k.a. very confusing, a.k.a. very real. What does this technical problem mean to the hazmat response infrastructure and the hazmat response mission? Potentially - a lot; Definitely - something. Y2k is a technical issue that has very real and very broad roots. However, it is also a program and resource management issue because it’s potential impact is far reaching and can compromise organizational and physical infrastructure at many levels. Every response organization has the potential for both internal and external Y2k vulnerabilities. If realized, these wide spread vulnerabilities could domino to stress the national response system and mutual aid network.

As a community, we plan and perform consequence management for weather disasters, earthquakes, oil spills, hazmat releases, terrorism events and other scenarios that can cause significant disruption and harm to human health, the environment and social infrastructure. We don’t know when these events will occur; we don’t know where they will occur; and we don’t know their size or impact. But we do know that there is a significant probability that something will occur, sometime, somewhere. So we plan for it. We must also plan for Y2k. The Y2k technology problem has the potential to cause significant disruption and harm to human health, the environment and social infrastructure. However, we know exactly when it will occur (January 1, 2000 and other associated dates); we know exactly where it will occur (everywhere) and although may not currently know the size or impact, we can get a good measure of it by assessing our internal and external vulnerabilities. As a community, responders, response planners, and response managers should all be well briefed on Y2k and prepared to deal with its consequences. The scope of this problem has yet to be completely defined, however significant, manageable effort can still be invested now to help control and minimize Y2k impact. Such efforts are critical in the emergency response community.

This white paper is structured to address Y2k issues in the same way that Y2k projects are organized : awareness, inventory, assessment, remediation, testing, and contingency planning. The awareness section will provide a brief education on the problem and its scope. The inventory & assessment section will provide a discussion on internal and external systems that are Y2k vulnerable and may affect the EPA removal program and its response capabilities. The remaining sections will be devoted to organizational discussions that include proposals for future work.

> As our Nation prepares for the year 2000 (Y2K), we face an urgent need to address the Y2K problem, which may cause computers and embedded systems that run America's critical infrastructure to malfunction or even shut down. With little over a year until January 1, 2000, this is a serious global challenge that businesses and governments around the world must address.
>
> **President Clinton**

> This is a management problem every bit as much as it's a technology problem. And the biggest mistake you can make if you are a CEO or a responsible manager is to say, 'My IT guy will fix this.'
>
> **Senator Bob Bennett**
> Chairman
> Senate Y2K Committee

> The Computer year 2000 problem, unless properly addressed, poses significant world-wide chemical safety problems.
>
> **International Forum on Chemical Safety**

> Francis Bradley, vice president of the Canadian Electricity Association said, "The lights will stay on" and "The bottom line is that most of the problems will be nuisance errors" such as "incorrect dates on logs, basically minimal problems that will not affect supplies to the consumers."
>
> **Wired News**

The problem is time..... There is not enough time to fix and test all the systems, with billions of lines of software code around the world, that need to be fixed. Many businesses, govern-ments, and organizations have become aware of the Year 2000 Problem only recently and may simply run out of time.

ED Yardeni
Chief Economist
Deutchbank Securities

There will be an estimated 25 billion chips at work on the planet on Jan. 1, 1999. Embedded systems far exceed the number of computer systems commonly considered to be the bulk of the Year 2000 problem.

Canadian Government's Y2k Web Site

Rohm and Haas, a Philadelphia based chemical manufacturer with US$4 billion in annual revenue, plans to shut down its plants in December 1999 to avoid Y2K glitches.

Wired News

Gartner Group, a Stamford, Conn.-based IT research company, said it has estimated the global cost of Y2K compliance at between $300 billion and $600 billion dollars.

TechWeb

National Association of Counties survey which showed that "only a total of half of the nation's 3,069 counties have begun addressing the problem."

Wall Street Journal

Our response obligations are fairly clear - we must be credibly educated on Y2k, get our own house in order, communicate with our response partners, and develop well-researched, realistic contingency plans and work around solutions. Time is short.

AWARENESS - i.e. PROBLEM DEFINITION

The Y2k technology problem has many aspects. Problem statements on the technical details, scope, and hazmat mission aspects of the issue are provided below:

problem statement- technical

Basically, the Y2k problem is caused by the representation of the four digit year (1970) as a two digit year (70). Even now dates are commonly represented in shorthand as MMDDYY. This abbreviation standard was developed to save on costly, limited computer memory in the early days of the computing era. It remained a standard for uniformity, simplicity, and just because. If a system element (e.g. microchip, software application) uses the two digit convention for dates and is date sensitive, the computer system will malfunction when it first encounters the date January 1, 2000. The system may recognize 00 as 1900, as an instruction signature, or as nonsensical data. Its malfunction may manifest itself in numerous ways including faulty data reporting and/or complete system failure and shut down. This is, technically speaking, a simple problem to fix. You must either reprogram or replace the vulnerable code or device. Easy? Unfortunately the answer is no. The impact and challenge of Y2k is found in its size, not in its technical detail. The sheer volume of work - inventory, assessment, remediation, testing - is enormous. In addition, the affected chips and software code can be difficult to find; they can be hard to evaluate; the fix must be tested; and time is short. Plus, most folks got a very late start in the game

<u>Myth</u>: Affected systems are exclusively defined as laptop, desktop, server, and mainframe computers and their associated software and hardware.

<u>Reality</u>: Affected systems include the embedded chip computers of simple devices that incorporate some sort of microprocessor for decision-making, data recording and/or function. While date sensitivity causes Y2k vulnerability, date does not have to be an obvious element of the microprocessor's function. Date stamping was often done automatically and as good engineering practice, regardless of chip function. In addition, many chips were manufactured generically with date functionality as a given. Y2k vulnerability is a function of chip specific design and application. By percentages

In general, there are two basic types of affected systems :

1. Information Technology (IT) - complex hardware and software computer systems.
2. Embedded Controls - simple microprocessors with "burned in" software code.

Because they are so pervasive and their date sensitivity can be difficult to grasp, it is worth expanding on the definition and Y2k impact of embedded controls a.k.a embedded systems.

According to the Institution of Electrical Engineers website on Embedded Systems and Y2k, "A general purpose definition of embedded systems is that they are devices used to control, monitor or assist the operation of equipment, machinery, or plant. 'Embedded' reflects the fact that they are an integral part of the system . . ."

An excerpt from the September 1998 NERC report to DOE illustrates the potential size of the problem:

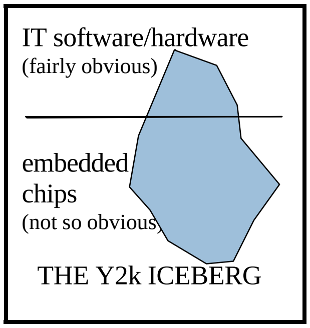
"In the electric industry, these chips are used in communications and numerous power system device controllers. Electronic chips are generally mass-produced without knowing the ultimate application of the chip. A single circuit board can have 20–50 of these chips from various manufacturers. Because of the diversity of chip suppliers, one vendor may use a different mix of chips even within devices labeled with the same name, model number, and year. Many of these chips have built in clocks that may experience date change anomalies associated with Y2k. The difficulty is in identifying all of these devices, determining if they have a Y2k problem, and repairing or replacing those that do. It is estimated that less than 1–2% of these devices may use a time/date function in a manner that could result in a Y2k malfunction of the device."

Although a 1- 2% Y2k malfunction rate may seem small, consider that there will be an estimated 25 billion chips at work globally on January 1, 1999. Two percent of 25 billion is 500 million. Other researched estimates of affected chips are based on a projection of 40 billion chips with a 1-10% rate of Y2k sensitivity. Either way, that is a large number of Y2k vulnerable systems that must be found, evaluated, fixed, and tested. If even a fraction of these chips have serious Y2k problems and even a fraction of them are infrastructure critical systems, the resultant problem could be sizeable though not necessarily unmanageable if adequate work is done in advance.

It is important to note that this is not just a January 1, 2000 issue. There are numerous dates that have the potential to affect computerized systems. This is important in planning as well as testing. A critical short list includes the following dates

April 1, 1999 - fiscal year start in some countries/states
April 9, 1999 - Julian calendar instance of 9999, a common instruction code signature
June 1, 1999 - fiscal year start in some countries/states
August 21, 1999 - GPS rollover
September 9, 1999 - calendar instance of 9999, a common instruction code signature
October 1, 1999 - fiscal year start for U.S.
January 1, 2000 - first instance of 00 as date
February 29, 2000 - non-standard leap year

problem statement - scope (i.e. affected systems)



THE Y2k ICEBERG

Until recently, the primary focus of Y2k remediation activities was software scrubbing and mainframe exorcizing. However, as the adjacent image illustrates, traditional computing and software systems (a.k.a. information technology or IT systems) only represent the tip of the iceberg where Y2k is concerned. Embedded systems represent a huge portion of the Y2k problem and can be present in the controls of everything from drinking water treatment plants, to fuel management systems, to fax machines, to pipeline SCADA systems, to manufacturing robotics, to chemical manufacturing systems, to power plant and power distribution systems, to communication equipment. As described by the Wired News report of the Chemical Safety Board's 12/98Y2k Summit, petroleum and chemical plants are laced with computerized control systems, some of which are vulnerable to Y2K glitches. Offshore oil platforms rely on automated controls to manage pumps, natural gas compressors, wellheads,

Los Angeles Police Department officials, taking no chances, have asked the mayor and City Council to set aside $4.5 million to keep as many as 300 more officers on patrol around the clock for a week before and after the turn of the century.

Los Angeles Daily News

We are increasingly confident that there will not be large-scale disruptions among banks and in the power and telecommunica-tions industries. Disruptions that do occur will most likely be of a more localized nature.

Quarterly Assessment President's Council on Y2k

One frustrating thing about the Committee that I chair is that as we probe in all of these areas -- and we've now held hearings virtually across the entire spectrum -- we still don't know. People lie to us. Or they refuse to talk to us

Senator Bob Bennett

California's welfare system runs through a network of local, state and federal computers. State officials are so concerned about a shutdown that the Health and Welfare Data Center plans to close its network on New Year's Eve 1999

Wall Street Journal

The Year 2000 Problem has clearly demonstrated the inter-connectivity and inter-dependency of the communications industry.

Michael K. Powell
FCC Commissioner

and air compressors. Every step of the oil delivery process -- production, processing, refining, and storage -- uses similar electronic controls. These embedded controls are numerous, wide spread and many may be affected by Y2k and other associated dates.

A few examples of Y2k sensitive IT and embedded systems is provided below. Attachment 1 provides a list of Y2k vulnerable systems at a generic waste water treatment facility. This list may also provide a good template for a generic chemical/petroleum manufacturing facility.

IT SYSTEMS	EMBEDDED SYSTEMS
FAA air traffic and control systems Rail yard and line switching systems SCADA systems in gas & petroleum pipelines 911 system CAMEO & Aloha ERNS Laptop/desktop/LAN operating systems Voice messaging system Inventory systems	Office automation (fax machines and photocopiers) Laboratory equipment Medical devices (including life support systems) Building infrastructure including HVAC & security Process control systems Electrical power generation and distribution systems Transportation and navigation systems Communication equipment Monitoring equipment

problem statement - mission

The hazmat and emergency response mission will most certainly be impacted by Y2k. The magnitude of that impact has yet to be completely defined. However, multiple or even single system failures could easily affect responders with impacts ranging from simple but pervasive "hassle factor" problems to significant safety, personnel and response problems. Even if there were no year 2000 technology problems, the social and community planning issues associated with the millennium change could impact the response community. Because EPA's response program provides support and back-up for local and state response capabilities, their Y2k problems may become ours. The fact that some urban police and fire departments are beginning to cancel leave for staff during the weeks before and after 01/01/2000 certainly illustrates the degree to which they expect their resources to be tapped. Indeed, it is possible that the whole of the mutual aid network may be challenged and stressed. This solid network may serve well when it is confronted with a handful of problems at the same time. But what if it is confronted with many significant response needs in many geographically disparate areas at the same time? What if it is confronted with these problems beginning in 1999 and well into the year 2000? Using worst case forecasting, the implications for the EPA emergency response program could include:

- Inability to communicate due to localized power, equipment, or telcom failures
- Response equipment failures
- Limited ability to travel due to transportation problems
- Increased reliance on EPA response support because local response capabilities are tapped
- Numerous infrastructure problems
- Equipment, personnel, and budget shortfalls
- Increased incidence in hazardous materials releases due to production facility Y2k problems
- Increased incidence in hazardous materials releases due to transportation Y2k problems
- Increased number of superfund/OPA clean-ups due to Y2k bankrupted facilities

While there is no degree of certainty that any one of these listed problems will occur, the potential is well-documented and is significant enough to warrant further investigation, evaluation, and planning. It is also important to note that there could be significant regional differences in Y2k vulnerabilities due to external factors like local infrastructure preparedness.

Management has to deal with it at a high level. This is about accessing risk and acting accordingly. Its impact will depend on the contingency plans that have been made.

Joseph Connor
United Nations
Undersecretary-General

Chevron in San Francisco does not anticipate Year 2000 problems to affect the importing of oil. However, the company will not operate vessels in restricted water, such as narrow passages or ports, on Dec. 31, 1999, because officials are concerned that on-board systems may receive contaminated data from systems that are not Year 2000 compliant

Federal Computer Week

For the last six months experts have been saying that nothing short of a Manhattan-type Project crash program can mobilize world opinion and world effort needed to address the Y2K problem in a way that minimizes damage.

Senator Sam Nunn

The Y2K problem is the electronic equivalent of the El Nino and there will be nasty surprises around the globe.

John Hamre
Dep. Secretary of Defense

It is not a question of one thing going wrong, it is a question of tens of thousands of things going wrong.

Arnaud de Borchgrave,
Center for Strategic and
International Studies

INVENTORY & ASSESSMENT - i.e. MISSION VULNERABILITY

What are the Y2k affected systems that can cause a problem for the EPA Removal Program and its response authorities, abilities, and obligations? In the construction of a laundry list of these vulnerable systems a pattern emerges illustrating that the systems generally fall into two categories: internal vulnerabilities and external vulnerabilities.

internal vulnerabilities

Internal vulnerabilities are those systems that are within the EPA removal program's span of control that may have Y2k problems. A partial list of potential internal vulnerabilities of the EPA removal program at a regional level include:

- response equipment (vehicles, monitoring & analytical equipment)
- communication equipment (fax, pagers, cell phones & service)
- field information technology equipment (laptops, gps)
- office IT equipment (LAN & associated desktops)
- physical infrastructure (building systems - including security & HVAC)
- personnel & funding availability - both EPA & Contract
- site engineered response systems (waste extraction, treatment, or monitoring)

IT systems and physical infrastructure systems are being addressed within each Region with HQ support. These activities have been underway for a while, so a good understanding of issues and the status of repairs should be easily acquired at a regional level. Each Region's Y2k coordinators should have the most updated information regarding these issues. However, regional Emergency Response Offices should confirm Y2k activities in their Region, both internally and externally. At present, the Y2k assessment of field equipment **-** including laptops, communication and general response equipment **-** is the responsibility of each Emergency Response Office. Regional organization may dictate otherwise, but until such support is confirmed, it should not be assumed.

external vulnerabilities

External vulnerabilities are defined as systems or organizations that may impact the hazmat response mission and /or infrastructure as a result of Y2k failures beyond the immediate control of the EPA removal program. These vulnerabilities are certainly more difficult to catalog and understand, much less address. However, a few broad category groupings can be identified for the purposes of this discussion. One must note in reviewing this list that failure or any dimension of impact on these systems is not a certainty. These are simply infrastructure areas that have been identified by a variety of analysts as being Y2k vulnerable. At a minimum, consideration should be given to each of these systems in contingency planning efforts. One should recognize that a great deal of private and public effort and talent has been and is being devoted to fixing Y2k problems in these systems. However, the problems are numerous and widespread and not all may be identified and/or fixed in time.

POWER	Potential for power disruptions and outages
TRANSPORTATION	Potential for transportation delays and/or disruption
COMMUNICATION	Potential for communication systems and equipment failures
SUPPLY CHAIN	Potential for delays in materials supply and distribution
WATER	Potential for disruption of drinking water supply
WASTEWATER	Potential for sewage treatment and processing failures
HAZMAT	Potential for hazardous material management/release problems
MEDICAL	Potential for medical equipment and device failures

There will be failures in the Americas, there will be failures in Europe and Africa, and Asia. There's not going to be anywhere where there are not going to be failures. And essential is that we accept the inevitability of some -- of quite a lot of failures; that we accept it. We don't know the degree, but that we are calm about this and that we prepare for disruptions to mitigate effects.

Maria Livanos Cattaui
International Chamber of Commerce

Dan Daley, maintenance director of Occidental. Chemical, said he found 3500 computerized devices in an ethylene plant his company owns, of which only 7 percent had Y2K problems.

Wired News

In the past three years, Pennsylvania has spent 1.3 million man hours and almost $40 million to deal with its Y2K problems. It now claims to lead all U.S. states in compliance.

Wall Street Journal

Alabama (claims to have finished none of its Y2K work so far) failed to allocate the needed $70 million last September, which caused Larkin Nolen, the state's CIO, to resign in protest.

Wall Street Journal

Chevron's third-quarter 10-Q warns investors that it may not be able to produce crude oil and natural gas as well as deliver refined gas to its customers.

Dow Jones Newswires

Y2k impact on most of the sectors listed above may not have a direct impact on hazardous materials response but may present response obstacles in the form of infrastructure failures and response resource diversion. Hazardous materials releases as an external vulnerability could result from chemical and petroleum manufacturing, storage, and transportation failures as a result of embedded control, software failures, or external factors such as power failures.

REMEDIATION, TESTING & CONTINGENCY PLANNING - i.e. FUTURE WORK

The amount of potential work that could be outlined in this section is large. One must identify issues broadly but prioritize and select the few that can produce results as quickly and as comprehensively as possible. The EPA Emergency Response Program should approach Y2k issues and readiness at many levels. All mission critical systems must be identified and evaluated. Such system evaluation should not be limited to information technology and equipment support, it should include response systems, networks, and protocols. Many aspects of the program may be affected from planning to field. A list of possible Y2k preparation activities for regional and national consideration is provided below as a template for further discussion and action. This list is followed by a very brief and by no means exhaustive discussion of activities that are currently underway in EPA's Emergency Response Programs.

NATIONAL LEVEL	REGIONAL LEVEL
Staff and Management Education on Y2k	Staff and Management Education on Y2k
Dedicated Y2k Planning and Outreach Staff	Identification of Y2k ER coordinator
Coordination of Task Force on Y2k Response Issues	Participation in Task Force on Y2k Response Issues
Development of Continency Plan Outline	Development of Regional Y2k Continency Plan
Development of Outreach & Educational Materials	Incorporate Y2k into ACP & RCP
Development of Equipment Checklist	Equipment Inventory & Assessment
Funding for Y2k Equipment Needs	Identification of Y2k equipment needs
Contracts Language and Support	START and ERCS outreach and coordination
Outreach to USCG & NRT	Outreach to Strike Team and other response partners
Coordination with EPA Y2k workgroup	Outreach to RRT, LEPC
Development of Y2k Work Plan	Communication with regional Y2k coordinator
Development of Inspection Inquiry Language	Incorporation of Y2k inquiry into inspections
Centralized Information Clearing House	Identify key Y2k personnel at State and Local levels
Outreach to Industry	Outreach to Industry

Numerous Y2k project activities are currently underway in the Emergency Response Program. These activities include but are not limited to:

- Monthly Conference Calls to discuss Y2k Project Status - HQ coordination
- Response equipment evaluation - Regional Coordination

The OERR monthly conference calls include the participation of regional emergency response representatives from the ten EPA Regions, as well as the Environmental Response Team. This group will monitor progress in the six steps outlined below to assure that EPA's domestic emergency response program is ready to maintain its responsibilities under the National Response System given the Y2k situation. Other stakeholders are also participating in these calls including the Technology Innovation Office, the Chemical Preparedness and Prevention Office, and the Office of Radiation and Indoor Air.

As additional efforts are undertaken, it is important that they be well organized and well documented. Successful Y2k programs will include the following steps:

With more than 44% of mission-critical components tested through November 30 1998, findings continue to indicate that transition through critical year 2000 rollover date is expected to have minimal impact on electric system operations in North America. Only a small percentage of components tested indicate problems with Y2k date manipulations. The types of impacts found thus far include such errors as incorrect dates in event logs or displays but do not appear to affect the ability to keep generators and power delivery facilities in service and electricity supplied to customers.

NERC January 1999
Report to DOE

The estimate for overall Coast Guard Y2K costs stands today at $34 million, including approximately $10 million already incurred through fiscal year 1998

Rear Admiral Naccara
U.S.C.G.

Information is crucial to our Nation's ability to successfully meet the challenges posed by the Y2K problem. People need to know what the problem is, how they can address it, and what governments and businesses are doing to ensure that their critical systems are ready for the new millennium.

John Koskinen
Chairman
President's Y2k Council

Airlines will spend $2.3 billion to fix millennium bug.

IATA Web Site

There is little point in our commiserating over how we have got into this situation, and why remedial actions have been so deeply delayed around the world. ..... Nor is there any point in trying to deliberate on the overall size of the Y2K problem, or to attempt to put a figure on the cost of remedial action. Irrespective of its size, this is a problem which just has to be solved. We all have a common stake in its solution, and that is all that need to be said about it.

Ambassador Ahmad Kamal
Chairman of the ECOSOC Working Group on Informatics

We are surrounded by evidence of Y2K. I can demonstrate specific systems which fail. I can demonstrate specific embedded system failures. I can point to the vast sums of money being spent by conservative companies to fix the problem. I can take you to the courts to listen to Y2K lawsuits. I can do all of this, but I cannot convince a cynical reporter that any of it exists.

Peter de Jager

We must be Paul Revere. We must tell everyone that Y2K is coming. But we must not be Chicken Little and tell them that the sky is falling.

Senator Bob Bennett
Chairman Senate Y2K Committee

One: Take Inventory

Designate a Y2k team leader. Make a list of equipment that may have Y2k problems. Consider computer systems, software programs, fax machines, monitoring equipment and other pieces of equipment that use embedded chips. Also consider support systems, such as building and security systems. As a parallel path, make an inventory of external Y2k vulnerabilities that includes contract, response, and communication networks. Such a list will serve as input in outreach and contingency planning efforts.

Two: Assess and Prioritize

List what you've done to prepare for Y2k. Identify equipment and systems critical to your operation. Make it a priority to fix or replace them, if appropriate.

Three: Evaluate and Test Your Systems

Evaluate and test your systems for Y2k problems. You should get educated on testing procedures before you begin. First, contact the equipment/software manufacturer directly. A tremendous amount of Y2k compliance status information is available on the web. However, while they provide a good degree of assurance you should not rely entirely on verbal or written assurances of compliance. You should also test your equipment directly, if possible. But be careful. Entering a Year 2000 date could shut it down. Follow the instructions of a reputable testing program or have an experienced tester perform this task.

Four: Correct Problems

Check out computer software or equipment upgrades to fix your Y2k problems. Contact software publishers. Ask what fixes or remedies they provide. After installing available Y2k fixes, retest your systems to verify that the fixes corrected the problem. Some equipment may need to be replaced. Don't forget to test your fixes as well.

Five: Make Contingency Plans

Develop contingency plans to address external and internal vulnerabilities, including a plan if you or your response partners have problems. Significant effort should be placed here and serious consideration should be given to exercises, communication strategies and resource needs, deployment, and pre-positioning. Can you get your troops & contractors out the door? Will they have the people, information, and equipment needed to work safely?

Six: Be Alert to Recontamination

Once you've completed your tests and fixed any Y2k problems, be careful not to recontaminate your systems by installing new programs or exchanging data with non-compliant systems. New equipment purchases and contracts should incorporate Y2k consideration.

Questions, Comments or Suggestions?

Several individuals within EPA's emergency response program may be contacted to discuss this paper. This version of the paper is dated 2/03/99. The originator and principal author is OSC Kay Lawrence of EPA Region IX. Kay may be reached at (415) 744 - 2289. The Senior Process Manager for Emergency Response within OERR is Mark Mjoness and the primary staff person at OERR is Regional Coordinator Dan Thornton. Mark and Dan may be contacted at (703) 603 - 8727 and (703) 603 - 8811, respectively.

ATTACHMENT 1

POSSIBLE LOCATIONS OF EMBEDDED CHIPS IN DRINKING WATER AND WASTEWATER TREATMENT FACILITIES

Communications Infrastructure

- Auto dialers
- Network bridge and routers
- Portable radio communication equipment
- Uninterruptible power supplies
- Wireless transmitters and receivers
- Voice/Data telecommunications equipment, including cell phones and pagers
- Uninterruptible Power Supplies

Instrumentation and Ancillary

- Automatic calibration systems
- Automatic sampling equipment
- Chemical analyzers
- Chemical feeders
- Hand held calibration equipment
- Lab and quality control instruments
- Maintenance diagnostic instruments
- Liquid flow meters (batch/totalizing)

Facilities and Support

- Battery chargers
- Building Heating, Venting, and Air Conditioning (HVAC) systems
- Building security systems
- Eyewash systems
- Fire and smoke alarm systems
- Programmable machining equipment
- Guard control systems
- Weather monitoring systems
- Uninterruptible Power Supplies
- Geographic Positioning System (GPS)
- Diagnostic Engine Analyzers
- Automated Fueling Systems

Materials Tracking

- Automated warehousing systems
- Bar code readers and printers
- Product/materials labeling and printing
- Wireless data terminals

Production and Process

- Automated reconditioning/ regeneration systems
- Distributed control systems
- Local controllers (programmable)
- Operator interface hardware
- Power monitoring equipment
- Programmable logic controllers (PLCs)
- Weight scales
- Demand management controls
- Hand held programming terminals and equipment
- Message displays
- Operator interface software
- Programmable chart recorders
- Data loggers
- Proprietary communications interfaces
- Supervisory Control and Data Acquisition System (SCADA) hardware and software
- Meter reading equipment
- Remote terminal units

Process Controls

- Flow meters
- Pump motor controllers
- Level controllers
- Flow controllers
- Chemical feeders
- Mixer speed controllers
- Aeration blower controllers
- Chlorinators